Amendments to the Claims:

1-14. (Cancelled)

15. (Currently amended) A digital right management system, comprising:

a secure component ~~container~~;

an ~~application programming~~ interface ~~which provides interface~~ between said secure component ~~container~~ and a ~~third party~~ software application;

said secure component ~~container~~ processes ~~the~~ requests coming from said ~~third party~~ software application through said ~~application programming~~ interface;

said secure component ~~container~~ validates signatures of one or more certificate documents to verify that said software application is ~~said one or more documents are~~ compatible with said secure component ~~container~~;

in the case of verification of compatibility ~~of said one or more documents with said secure container~~, said secure component allows operation of said software application ~~container initiates loading one or more dynamically linked libraries~~; and

in the case of incompatibility ~~of said one or more documents with said secure container~~, said secure component ~~container~~ refuses to ~~load any data coming~~ allow operation of said software application through said ~~application programming~~ interface.

16. (Currently amended) A digital right management system according to claim 15, wherein said ~~third party~~ software application comprises a rendering engine.

17. (Previously presented) A digital right management system according to claim 16, wherein said rendering engine is connected to a printer.

18. (Previously presented) A digital right management system according to claim 16, wherein said rendering engine is connected to a computer monitor.

19. (Previously presented) A digital right management system according to claim 16, wherein said rendering engine is connected to a handheld device.

20. (Previously presented) A digital right management system according to claim 16, wherein said rendering engine is connected to a wireless device.

21. (Previously presented) A digital right management system according to claim 16, wherein said rendering engine is connected to a device with one or more optical communication ports.

22. (Currently amended) A digital right management system according to claim 15, wherein said secure component ~~container~~ performs rights management.

23. (Previously presented) A digital right management system according to claim 15, further comprising one or more self-protecting documents.

24. (Previously presented) A digital right management system according to claim 15, further comprising one or more structured storages.

25. (Previously presented) A digital right management system according to claim 15, further comprising one or more structured file systems.

26. (Previously presented) A digital right management system according to claim 15, further comprising information specifying content types.

27. (Previously presented) A digital right management system according to claim 15, further comprising information specifying licenses.

28. (Currently amended) A digital right management system according to claim 23, wherein said secure component ~~container~~ detects whether any of said one or more self-protecting documents is tampered with.

29. (Previously presented) A digital right management system according to claim 15, further comprising an encryption engine.

30. (Previously presented) A digital right management system according to claim 15, further comprising a user-interface module.

31. (Previously presented) A digital right management system according to claim 30, wherein said user-interface module includes one or more menus or toolbars.

32. (Currently amended) A digital right management system according to claim 15, wherein said secure component ~~container~~ acts as a shell to be compatible to ~~the third party~~ plug-ins which are designed based on a predetermined specification of said secure component's ~~container's~~ interface.

33. (Previously presented) A digital right management system according to claim 15, further comprising a software development kit that enables the creation of applications to protect, distribute, and consume content.

34. (Previously presented) A digital right management system according to claim 15, wherein said system is connected to one or more storefronts.

35. (Previously presented) A digital right management system according to claim 15, wherein said system is connected to one or more backoffices.

36. (Previously presented) A digital right management system according to claim 15, wherein said system creates one or more rights labels.

37. (Previously presented) A digital right management system according to claim 15, wherein said system creates one or more rights templates.

38. (Previously presented) A digital right management system according to claim 15, wherein said system creates one or more metadata.

39. (Currently amended) A digital right management system ~~comprising:~~ according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said ~~a third party~~ software application;

said secure environment processes the requests coming from said ~~third party~~ software application through said application programming interface; and

said secure environment validates one or more documents.

40. (Currently amended) A digital right management system ~~comprising:~~ according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said ~~a third party~~ software application;

said secure environment processes the requests coming from said ~~third party~~ software application through said application programming interface; and

said secure environment validates one or more documents to verify that said one or more documents are compatible with said secure environment.

41. (Currently amended) A digital right management system ~~comprising:~~ according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said ~~a third party~~ software application;

said secure environment processes the requests coming from said ~~third party~~ software application through said application programming interface; and

said secure environment validates signatures of one or more documents to verify that said one or more documents are compatible with said secure environment.

42. (Currently amended) A digital right management system ~~comprising:~~ according to claim 15, wherein said secure component comprises a secure container;

said interface comprises an application programming interface which provides interface between said secure container and said ~~a third party~~ software application;

said secure container processes the requests coming from said ~~third party~~ software application through said application programming interface; and

said secure container validates signatures of one or more documents to verify that said one or more documents are compatible with said secure container.

43. (Currently amended) A digital right management system ~~comprising:~~ according to claim 15, wherein said secure component comprises a secure repository;

said interface comprises an external interface which provides interface between a processing means and an external environment;

said secure repository processes requests for access to a digital work; and

said secure repository checks usage rights, and after checking, grants the access to said digital work.

44. (New) A digital right management system according to claim 15, wherein said secure component comprises one of a secure container, a secure environment, and a secure repository.

45. (New) A digital right management system according to claim 15, wherein said interface comprises an application programming interface.

46. (New) A digital right management system according to claim 15, wherein in the case of verification of compatibility, said secure component initiates loading of one or more dynamically linked libraries.

47. (New) A digital right management system according to claim 15, wherein in the case of incompatibility, said secure component refuses to load any data coming through said application programming interface.